High Level Architecture

Federation Security Process

Version 1.2

February 16, 2001

DMSO

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (FROM - TO)
16-02-2001		xx-xx-2001 to xx-xx-2001

4. TITLE AND SUBTITLE
High Level Architecture Federation Security Process. Version 1.2
Unclassified

5a. CONTRACT NUMBER
5b. GRANT NUMBER
5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER
5e. TASK NUMBER
5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME AND ADDRESS
Defense Modeling and Simulation Office
1901 N. Beauregard St., Suite 500
Alexandria, VA22311-1705

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS
United States Department of Defense
Defense Modeling and Simulation Office
1901 N. Beauregard St., Suite 500
Alexandria, VA22311-1705

10. SPONSOR/MONITOR'S ACRONYM(S)
11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APUBLIC RELEASE
,

13. SUPPLEMENTARY NOTES

14. ABSTRACT
The High Level Architecture (HLA) allows the assembly of different tools to address a requirement. The requirement may arise from the examination of an analysis problem; research and development explorations; test and evaluation of an object, component, or a process; or the provision of training to individuals or staffs. The HLA allows this requirement to be met by assembling an appropriate set of models, simulations, and other tools. Once identified, the challenge is to employ each model, simulation, or tool in a way that takes advantage of its strengths and complements the application of the other selected tools to meet the requirement. When assembled, the models, simulations and tools compose a federation; the individual components, called federates.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE	Public Release	54	Fenster, Lynn lfenster@dtic.mil
Unclassified	Unclassified	Unclassified			19b. TELEPHONE NUMBER International Area Code Area Code Telephone Number 703767-9007 DSN 427-9007

TABLE OF CONTENTS

TABLES AND FIGURES

FEDERATION SECURITY PROCESS

I. Introduction to the FSP

1. Purpose

The purpose of this Federation Security Process (FSP) document is to support integration of Automated Information Systems (AIS) security into the Defense Modeling and Simulation Office (DMSO) High Level Architecture (HLA) Federation Development and Execution Process (FEDEP). The Department of Defense (DoD) Information Technology Security Certification and Accreditation Process (DITSCAP), DoDI 5200.40, is a DoD approved process that standardizes the security Certification and Accreditation (C&A) process for DoD automated information systems. The National Security Telecommunications and Information Systems Security Committee (NISTISSC) has developed NSTISSI No. 1000, the National Information Assurance Certification and Accreditation Process (NIACAP) for national level efforts. The DITSCAP/NIACAP has been selected as the process to be used when applying and integrating applicable information security measures into the FEDEP.

This document only applies to federation development that must conform to the United States National or Defense level instructions. All creators of federations should consider security concerns of their respective owners. Good security and development practices should go hand-in-hand. The processes in the FSP, FEDEP and DITSCAP/NIACAP documents are all modifiable to allow differing development styles such as rapid prototyping.

The integration of security into the FEDEP should be considered the norm, rather than the exception. Mapping DITSCAP requirements and processes into the HLA FEDEP was the basis for development of the FSP. The FSP is a guide to integrating timely resolution of information security requirements and functional implementations into the life cycle process of federation development. It provides a framework for efforts involved in the practice of information security, such as risk management, security engineering, and determination of levels of assurance. The focus of the FSP is the production of a federation that contains sufficient security features and functions to allow the federation to operate securely.

The goal of this document is to map corresponding phases and activities of the DITSCAP into the FEDEP. Even though the FEDEP outlines some security concerns to be addressed when developing a ‘secure federation’, it does not provide the level of detail that is needed to enable federations to meet the requirements for security C&A. The FEDEP does not take into account federation security for federations that are not designated ‘secure federations’. This FSP does consider security for all federations and should be used for all federation development, whether secure or not. There are always security concerns for systems, even when they are unclassified. The DITSCAP analysis is used to determine the level of certification required by the federation. Unclassified and

classified federations require security measures to be documented and implemented based on the analysis of system requirements. The FSP treats all federations alike and is tailorable for all possible federation security requirements.

Security C&A ensures that systems are built that minimize the threats and vulnerabilities to a manageable level; to attain the lowest possible risk; and minimize the threat or vulnerability. The DITSCAP ensures that confidentiality, integrity, availability and accountability of the AIS have been considered.

The FSP serves to make one aware of phases in the DITSCAP that correspond to steps of the FEDEP. It is the responsibility of the federation team and the Security Engineer to follow the DITSCAP phases to develop a strong security posture during the federation development and execution process. Therefore, the federation team must gain an understanding of the applicable DITSCAP phases and activities that correspond to the FEDEP steps. In addition, the federation team must consider the issues of personnel roles and the certification level. Addressing security requirements and involving key players early in the life cycle of system definition and development minimizes the tasks required to facilitate security C&A of federations. The federation team needs to consider where personnel roles defined in the DITSCAP support the FEDEP and what level of certification is being pursued. Refer to the DITSCAP Application Manual, DoDI 5200.40-M, for a determination of the level of certification required by a system and for a description of the personnel roles and their functions. The determination of the certification level helps to identify the appropriate level of effort, focus the C&A analysis and testing, define the skills needed to perform the analysis/testing and define the documentation required.

This FSP was written for those involved with HLA federations created using the FEDEP. They should be familiar with the HLA FEDEP and be aware of security concerns regarding the development of HLA federations. Security personnel should be familiar with the DITSCAP Instruction and Applications Manual listed in the References section of this document.

2. Scope

The Federation Security Process is to be used by all federation team members and contains information that allows the security architecture to be created in conjunction with the federation it supports. It is not meant to provide specific details about the security C&A process; rather is it intended to indicate the type of security actions necessary to create and maintain the security posture, and the documentation which is to be produced at appropriate points in the federation definition, design, development, integration and execution processes. The process described in this document is intended to provide a framework in which to address the security aspects of federations, with a goal of security C&A. The information in this document represents suggestions of applicable practices, not requirements. The FSP encompasses all aspects of system development while integrating security requirements in the systems objective definition step and continuing

the security process through to a successful security accreditation and approval to operate for an operational system.

3. Document Organization

This document relates the DITSCAP phases and tasks to the FEDEP Steps. Knowledge of the FEDEP is assumed. This document was written to assist the developers in security matters and does not proscribe solutions, it only provides a recommended (standardized) process to follow.

Further information is available by reading the referenced documentation contained in Appendix A. Flowcharts of each phase are contained in Appendix B to assist in understanding the DITSCAP. Roles and responsibilities of DITSCAP players are listed in Appendix D. A sample SSAA is contained in Appendix F.

II. Processes Involved

4. FEDEP

The HLA provides a set of rules, an interface specification, and an object model template (OMT) to assist disparate simulations, models, and/or live systems in seamless integration into one environment. The process that supports this integration is defined in the FEDEP. The FEDEP shows users, system managers, federation implementers, data analysts, etc., the steps involved in the integration process, from concept to post-execution analysis. While it has distinctly HLA language in it, it really represents the best practices for putting together a distributed simulation. The FEDEP can be tailored to the specific federation development and execution to which it is being applied.

The FEDEP is designed to be a 6-step process for development of a federation. This process is shown in Figure 1. Each of the steps has numerous associated tasks. These tasks are detailed in the HLA FEDEP Model documentation. Likewise, the FSP can be tailored to the specific federation development and execution to which it is being applied.

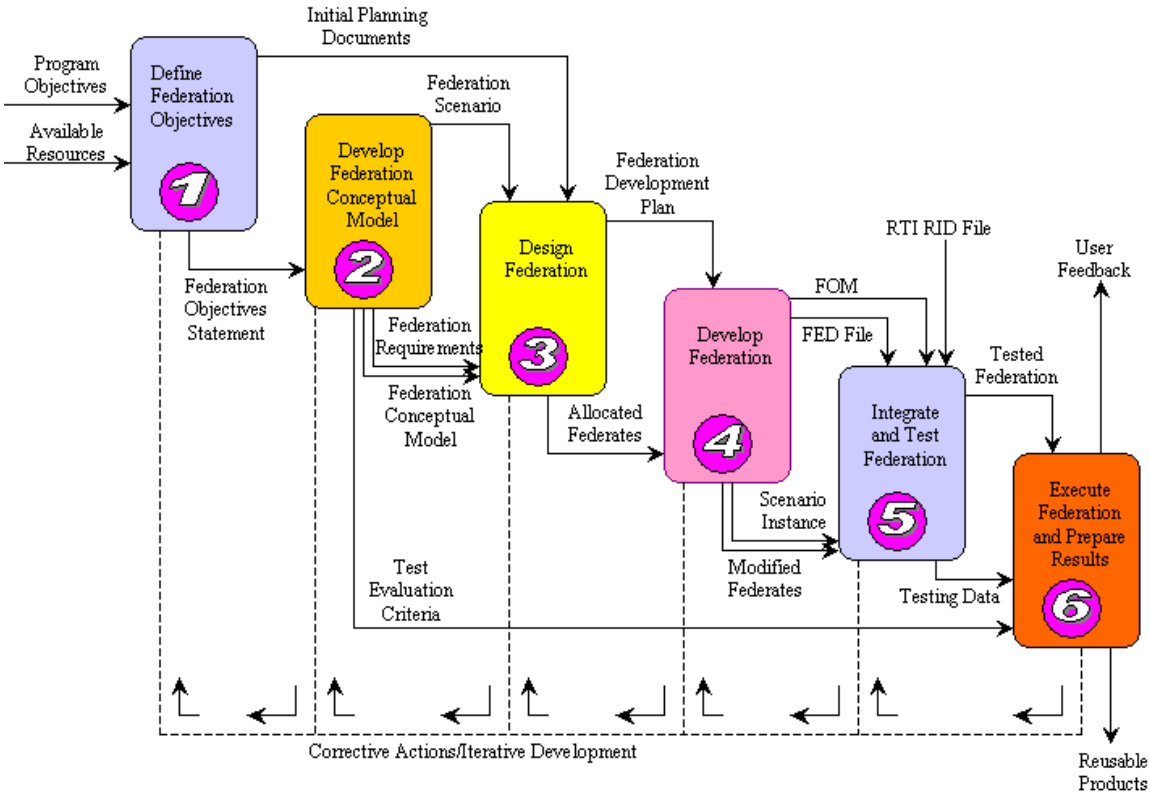


Figure 1: FEDERATION DEVELOPMENT AND EXECUTION PROCESS

Regardless of the reason for individual systems (simulations, models, live-systems) to come together, the fact that they can easily integrate with one another into one federation using the HLA provides a large and powerful tool in the modeling and simulation

inventory. As familiarity with the HLA increases, its application, and the systems that come together to support the application increase. As the variety of integrated systems increases, the differences to be overcome increase.

One major difference to overcome is that of differing levels of security. While it is possible that all the integrated systems have the same security level and require the same level of protection, it is equally possible that they do not. The need to ensure protection of the data and systems that have been integrated exists. In addition, the ways in which security can be applied to the integration process should be available to, and understood by, all members of the federation team.

5. DITSCAP

In much the same way that the FEDEP is a common, generalized way to view the integration of disparate systems into a seamless environment, the DITSCAP is a standard method used to provide security C&A of information technology systems. The DoD Chief Information Officer (CIO) Guidance and Policy Memorandum No. 6-8510 states that the DITSCAP is "The standard DoD approach for identifying information security requirements, providing security solutions, and managing information system security activities". Like the FEDEP, the DITSCAP is tailorable, and cyclical, and geared toward success. An Application Manual for applying the DITSCAP accompanies the DITSCAP Instruction. Figure 2 shows a high level representation of the DITSCAP.

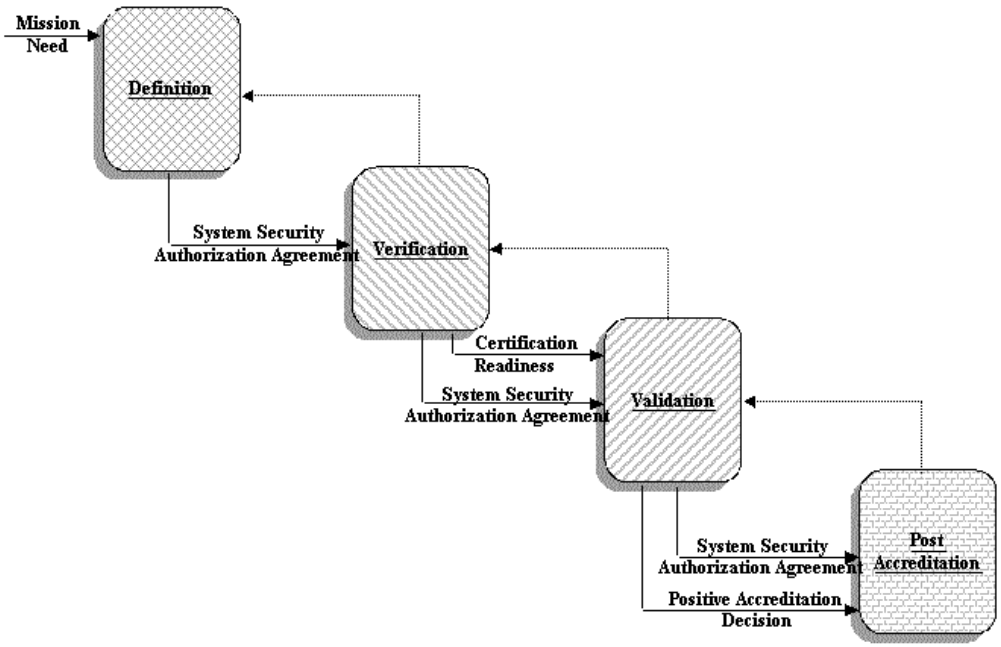


Figure 2: DEPARTMENT OF DEFENSE INFORMATION TECHNOLOGY SECURITY CERTIFICATION AND ACCREDITATION PROCESS

The DITSCAP requires the production of a System Security Authorization Agreement (SSAA) that has the following characteristics:

- Describes the operating environment and threat.
- Describes the system security architecture.
- Establishes the C&A boundary of the system to be security accredited.
- Documents the formal agreement among the Designated Approving Authority (DAA), Certification Authority (Certifier), user representative, and program manager.
- Documents requirements necessary for security accreditation.
- Documents security criteria for use throughout the Information System (IS) life cycle.
- Minimizes documentation requirements by consolidating applicable information into the SSAA (security policy, concept of operations, architecture description, etc.).
- Documents the DITSCAP plan.
- Documents test plans and procedures, certification results, and residual risk.
- Forms the baseline security configuration document.

The SSAA is a living document of federation security posture and contains all information related to the security of the federation being described.

The DITSCAP is subdivided into phases and tasks associated with each phase. A summary of the tasks is included in Appendix E. The DITSCAP Application Manual contains a more detailed description of each task. These tasks are numbered using the phase number followed by a hyphen and then the sequential task number within the DITSCAP phase (i.e. Task 1-1 is Phase 1 Task 1). At the conclusion of each task, a portion of the SSAA is completed (or updated) or an action is required before proceeding to subsequent tasks.

6. FSP

The FSP describes a security management process that is anchored in both the HLA FEDEP and the DITSCAP. The FSP provides guidance for the user to:

- Identify federation development and security professional participants and responsibilities.
- Identify the DAA or their authorized representative.
- Identify the Certifier and their role in the C&A process.
- Determine the component parts of the SSAA.

This guidance directs the development of the federation so that security can be applied and monitored throughout the subsequent phases of the DITSCAP. The specific guidance identified above belongs to Phase I of the DITSCAP and are used to start the security planning and implementation processes. The guidance provided by this process will assist

in defining security requirements for federations and allow the security analysts to provide any security mechanisms required. The process does not provide solutions, it is only a process used to define and mitigate security vulnerabilities.

The FSP products are produced at the appropriate time in the development process, not as an afterthought or sooner than feasible. By following the FSP, the federation can be ready for the security C&A process before the actual execution of the federation.

This FSP is designed for all members of the federation team. It contains information to allow the security architecture to be created in conjunction with the federate or federation it supports. It is not meant to provide specific details of the security C&A process; rather is it intended to indicate the type of security actions required and any documentation that can be produced at each of the stages of the FEDEP. The information in this document represents applicable practices.

To be useful and viable, a security process must be merged into the process of forming and executing a federation. The integration of security into the FEDEP should be considered the norm, rather than the exception. In addition, all aspects of security should be addressed as the federation development process proceeds. Overlaying the steps of the DITSCAP on the FEDEP, as shown in Figure 3, provides a high level overview of the FSP.

The objective of the FSP is to make the security processes, needs, and concerns, an integral part of federation development. This allows the identification, evaluation and elimination of security concerns as early as possible in the federation development and execution process, while it is still relatively simple to do so. The general principles that form the FSP are:

- Information security concepts must be applied to the federation development process to ensure that sensitive data is protected.
- The process must be integrated with the tasks of the FEDEP to allow security issues to be resolved in a timely manner.
- The design and development of the security mechanisms, safeguards, and procedures used in the execution environment are the result of the security engineering activities of the entire process.
- Allow the reuse of products in the FEDEP.

As seen in Figure 1, the FEDEP consists of six major steps while the DITSCAP consists of four major phases. The four phases of the DITSCAP have been spread over the six steps of the FEDEP, as shown in Table 1, to create the FSP steps required to implement security in HLA federations.

FSP STEP	FEDEP STEP	DITSCAP PHASE
1. OBJECTIVES/REQUIREMENTS DEFINITION	1. OBJECTIVES DEFINITION	1. DEFINITION
2. CONCEPTUAL MODEL DEVELOPMENT AND CONTINUED SECURITY DEFINITION	2. CONCEPTUAL MODEL DEVELOPMENT	1. DEFINITION
3. FEDERATION DESIGN AND SECURITY VERIFICATION	3. FEDERATION DESIGN	2. VERIFICATION (OF SECURITY)
4. FEDERATION DEVELOPMENT AND CONTINUED SECURITY VERIFICATION	4. FEDERATION DEVELOPMENT	2. VERIFICATION (OF SECURITY)
5. FEDERATION INTEGRATION AND TEST; SECURITY VALIDATION	5. FEDERATION INTEGRATION AND TEST	3. VALIDATION (OF SECURITY)
6. EXECUTE AND PREPARE RESULTS; POST (SECURITY) ACCREDITATION	6. EXECUTE AND PREPARE RESULTS	4. POST (SECURITY) ACCREDITATION

Table 1: FSP STEPS - MAPPING FEDEP STEPS TO DITSCAP PHASES

Specific information about these steps, tasks associated with each step, and security architecture creation and support can be found in subsequent sections of this FSP and in documents contained in the references section at the end of this document.

7. Tailoring

Tailoring is the process of examining each step and determining the extent to which it is needed in the process. Tailoring examines the critical issues and decisions necessary to provide the appropriate level of effort required to perform the security C&A. Likewise, tailoring optimizes the activities to make the most of the available resources, eliminating tasks that do not add value to the process or ultimate product. Unnecessary tasks add additional costs and delays to the federation development process.

Like the FEDEP and DITSCAP, the FSP covers the entire development and operational process, from definition through retirement, and is tailorable. The amount and scope of FSP work to be accomplished is different for a collocated federation with no external connections vice a geographically distributed federation. Like the FEDEP and DITSCAP, the FSP is not linear. It is possible to re-enter the FSP, as in the FEDEP and DITSCAP, if steps need to be repeated or added. When re-entering the FSP, the process flow must be followed. The FSP steps are organized in a structured manner to be followed in the documented order.

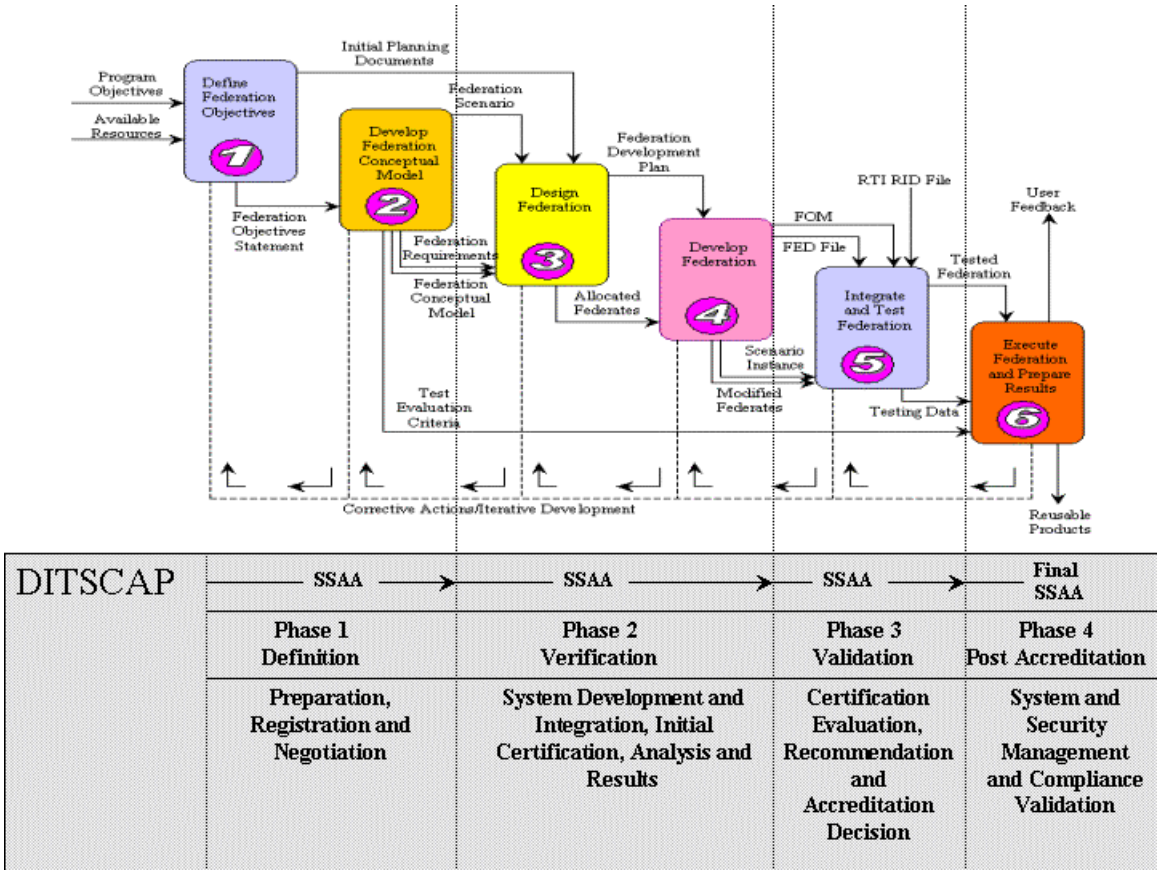


Figure 3: FEDERATION SECURITY PROCESS

8. FSP Current Technology Trends

Current technology allows the federation to operate at system high, using a Memorandum of Agreement as the primary vehicle for security agreements between each federate/federation. Requiring all federates within a federation to operate at a particular security level can place additional burden on some or most of the federates. Typically, if a federate operates outside the level of the federation, the burden of coming to the same level becomes the burden of the federate, either by adopting the level of the federation, or using a one-way or possibly two-way guard. This current capability should not dissuade the federation from completely working through the FSP. Just as technology is changing, so too are the security requirements of the federates and their components. In addition, as the federation development proceeds, new requirements or constraints may be revealed which make a single security level impractical; or a multiple level security federation unnecessary. The security needs must be examined as carefully as the technology needs to ensure that resources are properly used and that the desired outcome of the federation execution is achievable.

III. FSP Steps

9. FSP 6 Step Process

The FSP steps have been matched up to existing steps in the FEDEP so that federation developers can easily follow the process. The DITSCAP phases have been overlaid on the FEDEP to provide the necessary security mechanisms for federation development and execution. The following sections are included to provide management and developers with detailed information pertaining to the DITSCAP inclusion in the FEDEP.

9.1 FSP Step 1 - Objectives/Requirements Definition

The first step of the FSP is Objective/Requirements Definition. This step includes the FEDEP Step 1 and the DITSCAP Phase 1. (Phase 1 of the DITSCAP continues through FSP Step 2 and is associated with FEDEP Step 2.) Activities associated with FSP Step 1 are very similar between the FEDEP and DITSCAP as described below. Refer to the appropriate appendices for additional information and details.

The first step of the FEDEP is the definition of federation objectives based on the identified needs of the federation. The federation sponsor produces a needs statement, which can vary in content and format. The more information that the federation sponsor can provide about the reason for this federation, constraints under which it must operate, and the desired result of the product, the more successful and simple the succeeding steps can be. As the federation team moves through this step, the objectives become more concrete.

Phase 1 of the DITSCAP (Definition) is for identifying the mission need for the federation and for documenting the functions that the federation is to perform, identification of the system environment and architecture, identification of threats, definition of the level of effort, and any known security requirements and constraints. In addition, and perhaps most important, it identifies and begins the dialog between the security representatives. During this dialog, an initial assessment of the security C&A process is made and agreed on.

The dialog between the security representatives can begin once the security points of contact are established. Since this is early in the federation development, not all of the participants may be involved, or even identified. However, it is likely that the sponsor has a security point of contact who is involved and who may have knowledge of security constraints that must be satisfied. The sponsor identifies a DAA who is willing and able to coordinate the security activities of all the participants, and who can make technical and programmatic determinations when security issues arise. This person must be in a position to have direct influence on the IS facility and equipment. Any facility or equipment not directly impacted by the DAA is considered an external interface and requires separate security C&A. The DAA identifies the agency or individual who is responsible for security accreditation (Certifier).

As the FSP proceeds, it may be necessary to explore a range of options to solve the security issues that arise. The practice of open dialog has a positive impact on the ability to successfully resolve the issues that arise in a manner that is acceptable to both the development side of the federation team and the security side. In addition, the examination of solutions to security issues may contribute to resolving some of the general issues of the federation. In all cases, it is important to maintain a record of the important aspects of the dialog, especially when decisions are reached. All documentation is important for a variety of reasons (reuse, legacy, re-visitation of issues, etc.) and is to be included in the SSAA as appropriate.

The sponsor must document the mission needs (or requirements). This document can be used to begin the DITSCAP at Task 1-1. Other material is reviewed in this phase of the FSP, if it is available. These materials can include system specifications, business case, architecture documents, design documents, user manuals, operating procedures, network diagrams, configuration management documents, threat analysis and federal and organizational Information Assurance (IA) security instructions and policies. As with the FEDEP, the more detail that can be provided, the easier succeeding steps will be. For the security process, it is desired that the following information appear in the mission needs statement:

- Federation mission capabilities and function
- Desired interfaces and data flows associated with the interfaces
- Information to be processed
- Operational organization supported and providing sponsorship
- Intended operating environment
- Operational threat
- Expected federation life-cycle
- Federation user characteristics
- Operational environment of any preexisting components of the federation
- Classification of the data to be transferred and collected

Federation mission and function provide the overall basis for the discussion between the federation sponsor, federation developers, and security personnel involved in the security accreditation of the federation. It is imperative that the security personnel involved keep the ultimate needs of the federation sponsor in mind as decisions are made. There may be times where the needs of the federation sponsor cannot be met with current technology. By keeping the mission needs in mind and maintaining an open dialog between all parties, these areas can be dealt with as early in the process as possible and modifications can be made to the federation needs without compromising the security objectives of the federation.

Each organization joining the federation and/or benefiting from the federation has the potential to bring a different security concern to the discussion. It is important to keep all

the potential security needs and concerns in clear view of all participants and to identify as early as possible all potential showstoppers.

The classification of the actual data to be transferred is identified. Constraints about the level of data to be transferred and collected are identified. One important issue to be considered is that of data aggregation; the aggregation of the data can be classified higher than the individual data components. During federation execution and data analysis (FSP Step 6), it is likely that there is a tremendous amount of data located in one place. Many security concerns center around what can be derived from the data instead of what is contained in the data. As early as possible in the definition phases data aggregation should be considered so that appropriate security mechanisms can be implemented.

One issue that affects the type of security accreditation given and the way in which the security accreditation tests are to be conducted, is the expected life cycle of the federation. The federation security posture must be maintained throughout the entire execution life. This is the difference between accrediting a federation for a variety of executions and accrediting a particular federation execution for security. Contributing to this decision is the classification of the data to be transferred and the federation user.

The federation development team must refine the needs statement into a set of more concrete objectives. Typically, this brings in additional members of the federation development team. This is the ideal time to conduct the Registration tasks associated with Phase 1 of the DITSCAP. Task 1-2 calls for preparation of the system and functional description, included as Section 1 of the SSAA, from the documents reviewed in Task 1-1. As the mission need statement is transformed into the more concrete objectives, the level at which the federation is expected to operate becomes clearer. This approach determines the minimal security requirements necessary to secure the federation. In addition, as the federation becomes more stable, what is actually considered in security C&A becomes more stable.

Task 1-3 assigns roles and begins the dialog between the federation developers and the sponsors' security team (or the sponsor and security representatives from pre-identified federates). Identification of the security representatives and identification of the DAA for the federation is critical to the success of the process. While it is certainly possible to proceed in both the FEDEP and FSP, it is risky to the success of the security C&A process to continue without these designated personnel. The security knowledgeable individuals from the federates involved, the sponsor, and the security Certifier have the know-how to assist in merging the technical needs of the federation with the security technology available. These individuals have the knowledge to understand how the operational environment is threatened. They need to work in close cooperation with the federation and federate developers as members of the same team. The FSP proceeds more smoothly if all decisions are presented to all members of the team, for each individual can contribute a unique perspective based on their area of expertise.

The DITSCAP defines personnel roles, their associated responsibility and tasks to be accomplished by personnel in each role. The roles in the DITSCAP are identified during Task 1-3. The roles to be performed in the FSP may be performed by one individual, many individuals, or one individual may perform multiple roles. As is often the case in security, there may be a technical person who is well versed in the security needs of the federate he/she is representing, in which case, there may not be a need for a separate security representative. In that case, the federate representative assumes the responsibility of relaying important information between the security representative and/or DAA of the federate, and the other federation members, so that they may be kept up to date on decisions, and may verify decisions that were made.

The DITSCAP generates a dialog between the information system program manager, DAA, Certifier, and user representative and results in an agreement on security issues. These individuals resolve critical schedule, budget, security, functionality, and performance issues. The SSAA is used to guide and document the results of their decisions and the expected impact on the C&A process. The objective is to use the SSAA to establish an evolving, yet binding, agreement on the level of security required before the system development begins or changes to a system are made. The SSAA is used throughout the entire system life cycle to guide actions, document decisions, specify IA requirements, document certification tailoring and level of effort, identify possible solutions, and maintain operational systems security.

The agreements to be documented in the SSAA are coordinated with all of the applicable federation development team members. The federation team includes the representatives outlined in both the FEDEP and DITSCAP. The SSAA plays the same role in the FSP as it does in the DITSCAP. After security accreditation, the SSAA becomes the baseline security configuration document.

The FEDEP personnel requirements can vary greatly depending on the scope of the federation application and the certification level of protection. In the case of federation development, highly integrated teams composed of several individuals may be needed to perform a single role in a large, complex federation, while a single individual may perform multiple roles in smaller applications. Examples of the types of roles individuals can assume during the FEDEP include:

- Federation user/sponsor
- Federation manager
- Technologists
- Security analysts
- Verification, validation, and accreditation (VV&A) analysts
- Functional area experts
- Federation designers
- Execution planners
- Federation integrators
- Federation operators

- Federate representatives
- Data analysts

Some roles (e.g., operators) are unique to a single activity in the federation development process, while others are more pervasive throughout the process (e.g., federation manager).

The FEDEP and the DITSCAP have roles that are represented in both processes. Hence, in the FSP, the federation development team members agree on how to integrate the roles in the DITSCAP into the roles that are represented in the FEDEP. Theses roles are discussed below.

The key roles in the DITSCAP are the program manager, DAA, Certifier, and user representative. Additional roles may be added to increase the integrity and objectivity of C&A decisions in support of the system business case or mission. For example, the Information Systems Security Officer (ISSO) usually performs a key role in the maintenance of the security posture after security accreditation. The DITSCAP approach allows you to adapt the DITSCAP roles into their respective organizational management structure to best manage the risks to their mission throughout the IS life cycle: system development, operation, maintenance, and disposal.

The DITSCAP defines specific roles to be assigned and the responsibilities associated with each of these roles as follows:

Program Manager - The program manager represents the interests of the system throughout its life cycle (acquisition or maintenance, life cycle schedules, funding responsibilities, system operations, performance, and maintenance). The organization the program manager represents is determined by the phase in the life cycle of the system.

Designated Approval Authority (DAA) - The DAA is usually a senior operational manager with the authority and ability to evaluate the mission, business case, and budgetary needs for the system in view of the security risks. The DAA must have the authority to oversee the budget and IS operations of systems under his/her purview. The DAA determines what is an acceptable level of residual risk and approves the system operation.

Certifying Authority (Certifier) - The Certifier (and certification team) provides the technical expertise to conduct the certification through the system's life cycle based on the security requirements documented in the SSAA. The Certifier determines the level of residual risk and makes a security accreditation recommendation to the DAA.

User Representative - The operational interests of the systems users are vested in the user representative. In the DITSCAP, the user representative is concerned with system availability, access, integrity, functionality, and performance in addition to confidentiality as they relate to the system mission.

Specific tasks associated with each of the DITSCAP roles are defined in the DITSCAP phases.

The Security Engineer is an integral part of the development process. This person is involved in development from initial system definition through the execution step. The Security Engineer assists the Program Manager and DAA in resolving security issues. The Security Engineer ensures that applicable security mechanisms are implemented and security related documentation is developed in the federation systems development process. The Security Engineer is also responsible for interfacing with the user representative and the programming staffs to ensure that security details are covered in the design of each federate within the federation.

Dialog is an important part of both the FEDEP and the DITSCAP and, consequently, the FSP. It has often been stated that the most difficult part of bringing any federation together is the cultural aspects; getting individuals to communicate is often more difficult than the technical challenges of the problem. That is certainly true during federation development, when all individuals are focused on the technical solutions. Now, there is another voice added to the equation – and that voice may not be technical in nature. The newest addition is that of secure development and operation of the federation. The technical members of the federation involved in the requirements definition step must be willing to listen to the security concerns and technical solutions to optimally design their requirements for a federation that can be security certified and accredited. This dialog occurs in both directions; the security voice must be willing to contribute, as well as listen.

The appropriate security requirements, needs and mechanisms can most correctly be determined by those persons responsible (data owners) for the technical information to be exchanged (i.e., those who can assess its value and threats against it).

It is important to realize that the intent of the FSP is not to build an incredibly large team. It is worth reiterating at this point (and at every step within this process) that one individual may perform one or more functions, or many individuals may be necessary to adequately perform one function. The roles an individual may take can cross disciplines; a federate representative may be well versed in the security needs of his federation, while a data owner may have to rely on other individuals for complete security information. Often, it is the security of the mission and its' requirements that is most complex vice the mission needs or objectives.

Task 1-4 is used to define the system environment and potential threats. The system environment includes facility security, physical security, administrative security, personnel security, COMSEC requirements, TEMPEST requirements, preventive maintenance and security training. This information is used to create SSAA Section 2.

In Task 1-5, the security representatives involved contribute towards identifying and understanding the security policies to be enforced. These directives and requirements can

come from a variety of interests: national, local, service, agency, data owners, etc. A tool was developed that provides an automated method of producing a Requirements Traceability Matrix (RTM). This tool is available on the Internet to .gov and .mil sites. See the RTM Users Guide for a link to this application and operating instructions. Once again, getting the knowledgeable individuals involved in the requirements definition step helps to ensure that these wide-ranging concerns are identified. SSAA Section 4 is produced to document system security requirements.

As documents are developed and information is presented, they should be gathered so that reuse can occur, and lessons learned and decisions can be captured. The DITSCAP identifies the SSAA as the designated repository for this information. The FSP adopts this idea; and considers it a virtual folder into which all information can be captured. It is the responsibility of the federation lead to keep this folder current. The SSAA is a living document that is maintained to reflect the status of the project. This document records the agreement of the key players in the FEDEP on the goals and level of effort anticipated in the project. The security details of the evolving project and the results of the analyses update the SSAA. The security accreditation package is formed by the recommendation, the supporting documentation and the updated SSAA. Based on the spirit of the DITSCAP, separate new documents need not be produced if this information is documented elsewhere.

At this phase, another key aspect of the SSAA is the life-cycle support plan. As with all plans, this is a living document, updated as the federation progresses. However, even at the start of federation development, the security team, as it is currently composed, works with the sponsor, and user if possible, to prepare a security plan which encompasses all phases of the federation – from current development work, through breakdown and dissolution of the federation. The plan ensures that any accepted federation security risk would not worsen and to allow for enhancements in the security of the federation, if required.

A measure of the value of the SSAA can be seen when one considers that at this stage of the FEDEP, the federation membership is far from complete or certain. Therefore, it is imperative that all decisions be captured, so that if the membership of the federation changes, all information of the current state of the federation security posture is available for all members in an unbiased presentation. The SSAA is updated whenever necessary. One rule of thumb is that no information should be left out. It is impossible to predict what the later stages of the federation development require in terms of the history of decisions that were made. In addition, the SSAA, as stated previously, is a part of the security accreditation package and it may be necessary for the DAA to research the current security posture of the federation. All of the research for the C&A process should be able to be done directly from the SSAA. The DAA, Certifier, user representative and program manager can tailor the content of the SSAA.

9.2 FSP Step 2 - Conceptual Model Development and Continued Security Definition

In the FEDEP, the second step is for conceptual model development, which consists of the interrelated tasks of conceptual analysis and scenario development. These tasks feed off one another, each being used to refine the other. Conceptual analysis considers the problem space and develops the conceptual representation of the federation objectives and constraints. The Federation Conceptual Model (FCM) is the creation of FEDEP conceptual analysis, which transforms objectives into functional and behavioral characteristics. It uses the federation scenario to identify objects, relationships, behaviors, and algorithmic relationships between objects

Scenario development considers the operational constraints defined in the objectives statement. During scenario development, capabilities, behavior, and relationships between entities are defined. Scenario development considers the FCM as a means to provide an object-based view of the real world domain. The product from this FEDEP activity is the Federation Scenario Specification (FSS).

It is during this step of the FEDEP, that the dialog between the security representatives of the federates and federation and the technical representatives of the federates has tremendous payoffs. The registration step of the DITSCAP is still occurring here, as the technical representatives are coming together, some for the first time. A clearer picture of the virtual operational environment for the federation is being defined as the details of the conceptual analysis and scenario development are worked out. Also, a better definition of the needs of the federates (possibly indicating a change to membership) is occurring. Choices are being made, which are dictated by the operational performance, feasibility, affordability, and sponsor/user preferences. These choices bring with them their own risks and must be carefully considered in the overall security posture of the federation.

One aspect of both the FCM and the FSS(s) to consider is that of the classification of these items. They are likely to have usefulness past the dissolution of the federation. Just as the scenario development efforts and conceptual analysis efforts draw on repositories, such as the Modeling and Simulation Resource Repository (MSRR) and Functional Description of the Mission Space (FDMS), it is likely that products created for a federation will be placed in the same or similar repositories. In such a case, careful consideration is given to the selection of entries and their operations. This may lead to a data aggregation problem, where it is not what can be determined from the entries themselves, but what can be assumed from the entire package. Security decisions such as these, which are dependent on operational considerations rather than the sensitivity of specific data being processed, are to be documented in the federation security policy and security concept of operations, to be included in the SSAA.

Task 1-6 calls for the preparation of SSAA Section 3 which is the System Architecture Description that includes a definition of the system hardware, software, firmware, interfaces, data flows and the security accreditation boundary. The security accreditation

boundary covers all systems that interface with the federation to perform the functions defined in the Functional Description and that the DAA has authority over.

Section 5 of the SSAA is created during Task 1-7 which identifies the organizations and individuals involved in the C&A process. In addition, it defines any resources and training requirements that are necessary for security of the federation.

The DITSCAP has four levels of certification to provide the flexibility for appropriate assurance within schedule and budget limitations. The DITSCAP certification tasks are performed at one of these four levels of certification. To determine the appropriate level of certification, the Certifier analyzes the systems business functions, national, DoD, and agency security requirements, criticality of the system to the organizations mission, software products, computer infrastructure, data processed by the system, and types of users. Considering this information, the Certifier determines the degree of confidentiality, integrity, availability, and accountability required for the system. Based on this analysis, the Certifier recommends a certification level. The determination of the certification level identifies the appropriate level of effort, where to focus the C&A analysis and testing, the skills needed to perform the analysis and the supporting documentation. The system being certified could range from a simple stand-alone personal computer to a large data center, or command and control system. It could be a simple LAN in a vault or a cross-country distributed wide area network. Throughout the C&A process, phases and activities remain the same for any of these systems, the level of analysis is tailored to the system. The four levels of certification are identified in Table 2.

Level	Certification Level	Description
1	Minimum Security Checklist	Level 1 requires completion of the minimum-security checklist. The system user or an independent certifier may complete the checklist.
2	Minimum Analysis	Level 2 requires completion of the minimum-security checklist and independent certification analysis.
3	Detailed Analysis	Level 3 requires completion of the minimum-security checklist and a more in-depth, independent analysis.
4	Extensive Analysis	Level 4 requires completion of the minimum-security checklist and the most extensive independent analysis.

Table 2: C&A CERTIFICATION LEVEL

The DITSCAP provides the ability to calculate the certification level of a federation using weighted values assigned to characteristics of the federation. These values are totaled to produce a number that can fall within a range of certification levels. This process is detailed in section C3.4.8.2.1 of the DITSCAP Application Manual and is performed in Task 1-8.

Certification Level	Weight
Level 1	If the total of the weighing factors are < 16.
Level 2	If the total of the weighing factors are 12 - 32.
Level 3	If the total of the weighing factors are 24 - 44.
Level 4	If the total of the weighing factors are 38 - 50.

Table 3: CERTIFICATION LEVEL WEIGHTS

The Certifier determines which level to certify the system based on the system characteristics and total weight values. Certification levels overlap and it is the responsibility of the Certifier to determine at which level the certification is to be done. See the "Sample Federations" in Appendix C for a complete explanation of the weighing factors.

The SSAA is assembled and completed in draft form (Task 1-9) for delivery to the DAA, Certifier, Program Manager and user representative for review. The draft SSAA establishes a reference for discussions during negotiation.

The final three tasks, identified as the 'Negotiation' process (Tasks 1-10 through 1-12), include the Certification Requirements Review (CRR), agreement on the level of effort and schedule for the C&A activities. This process concludes with the approval of the Phase 1 SSAA by the four principal proponents of the SSAA (Task 1-12).

As the dialog between the federation team members (including security representatives) deepens, negotiation takes place, enabling agreements in both the security level and the technical aspects to be reached. Any issues which are not resolved, either in this step, or in others, are likely to cause problems in the security C&A. At this point, the security representatives are able to indicate new technologies that have a positive impact on these unresolved issues and in what situations they are approved for use. Often, benefits accrued from use of a new technology outweigh the programmatic and technological risks added by relying on it. However, it is only if all parties are fully aware of the issues which caused this choice, the background, and the desired end result that an informed, proper decision can be made for the federation.

During negotiation, the SSAA is reviewed for completeness and currency. At this point it is likely that the SSAA contains information such as MOAs, a concept of operations, federate security policies, surveys of existing security technologies, and rationale for security decisions. In addition, during negotiation, the FSP tailoring is updated, the security level is set and the certification requirements are drafted. (These are to be added to the relevant sections of the SSAA.) A key element of selecting the security level is the agreement on common need-to-know and releasability requirements for data to be shared among the federates. This does not mean that the security level and C&A requirements and plans are determined and cast in stone. Rather, it is to ensure that all federates understand the federation security requirements completely and that these are properly

captured in the SSAA. Since it is possible that the federation is being built from the bottom up, it is easier to ensure that the collection of federates selected have security processes and technology that meet the federation security level needs. For those federates which are being composed for this federation, technology can be applied and taken advantage of, to the collective benefit of the federation.

Security C&A is only one part of a federation transition to operation and support. In particular, The DITSCAP defines security certification as the "comprehensive, independent assessment of technical and non-technical security features and other safeguards of a [federation] to establish the extent to which a particular [federate] meets a set of specified security requirements for its use and environment." Security accreditation as defined by the DITSCAP is the "formal security declaration by a DAA that a [federation] is approved to operate in a particular environment using a prescribed set of safeguards, and is strongly based on the residual security risks identified during certification. The DAA has the formal responsibility of authorizing security relevant operation of the system." Items which may be additionally developed during this step, and possibly used as input to the C&A are the security objectives and requirements, security assurance plans, threat analyses, security related design information, life-cycle support plans, risk assessment, and applicable security profiles of the identified federates. Whether or not these items are developed is a decision of the federation security team. Typically, these individuals may be composed of federation team members who also have technical positions and can make an early determination as to how much information is needed for a complete security C&A program. It is important to remember that the security risk to a federation does not remain constant over time, especially if persistent federates are being reused. Since it is changing, the DAA remains actively involved (either directly or through some appointed federation member) during the entire federation life cycle.

9.3 FSP Step 3 - Federation Design and Security Verification

By using/reusing the previously developed FCM and FSS, the membership of the federation is more firmly established. It is likely that some federates were identified early in the FEDEP. Indeed, these early members are what enabled the security process to be given a strong boost. However, now that the entities and their behaviors and relationships are established and the objectives are understood, the membership is confirmed. In addition, all members verify that they can perform the work expected of them and that all necessary functionality is covered.

Equally important as the federate technical functionality, is that of security functionality. The security posture that the federate brings to the federation, or is willing to assume based on its membership in the federation, must be understood by all members of the federation development team and accepted by all. New members' security representatives can review the information in the SSAA to become acquainted with the history of the current state of the security needs of the federation. Remember that the SSAA is a living document. As the federation design activity continues, the SSAA is updated with the architecture of the federation, network connectivity information, integration and use of

off-the-shelf products, designs from software and hardware modifications, and anything else that affects the federates or the federation.

Phase 2 of the DITSCAP (Verification) can start. Phase 2 begins with a refinement of the SSAA, continues with federation development and completes with an initial certification analysis and results analysis. The purpose of this phase of the DITSCAP is to verify that the information contained in the SSAA complies with the federation as designed and developed, to analyze the life cycle management process, to validate security requirements, to create test plans, to create test procedures, and to assess the vulnerabilities against the countermeasures. The Minimal Security Activity Checklist is a standardized questionnaire used to ensure that analysis of developed products is consistent and complete. This checklist is contained in Appendix 2 of the DITSCAP Application Manual and is used throughout DITSCAP Phases 2 through 4. The checklist is broken down into sections to be accomplished during each of the tasks in these phases.

Federation design is another activity that benefits from the close dialog between the technical representatives, federation development team, and the security representatives. As the federation is molded, modifications may need to be made to the federates themselves. Sometimes, these modifications may invalidate the current security accreditation which each individual federate brings to the federation. The security representatives can help the technical representatives identify these cases and can help select alternatives which may not be as damaging to the security accreditation, if alternatives exist. Likewise, the security representative is able to approximate the amount of work involved in reaccrediting the modified federation. In addition, since this is now a functional team, other technical and security representatives may have alternatives not thought of by the federate representatives.

It is important to remember that even though this document speaks of security decisions separately, security of the federation is an integral part of the overall federation design (there is one design for the federation). The security team makes a valuable contribution to that design. Each federate is responsible for a particular aspect of the federation and each federate is responsible for a particular aspect of the security of the federation.

Federation design also produces a roadmap to federation development and integration. Part of this roadmap includes the vulnerability analysis and risk assessment for the C&A process. The federation is reviewed and compared against the information and documentation in the SSAA. This review determines if the federation is on-track for a successful C&A. It identifies where documentation is incomplete, out of date, or does not match the intended operation of the federation. The review also ensures that an overall security level is determined which is consistent with the objectives that were initially identified for the federation and environment in which the federation is executed.

9.4 FSP Step 4 – Federation Development and Continued Security Verification

Step 4 of the FEDEP is that of federation development. During federation development, the Federation Object Model (FOM) is created. The complication for federations is that the FOM must be effective, without compromising the protection of the information being processed. It may be possible to reuse both an existing FOM, either in whole or in part, as well as the existing FOM security information. However, it must be reviewed for currency and possible application of new technologies that may not have been available when the original item was created or used. Regardless of the methodology used to create the FOM, it is imperative to remember that data that becomes part of the FOM is freely accessible to all members of the federation (as per the HLA rules). The security level of the federation as specified in the SSAA is reviewed with this in mind. The federation security level accounts for the objectives and content of the overall FOM, the effects of reuse of existing SOMs and FOMs, data aggregation, and analysis data created and collected. If a given federate contains data with restrictions that are not within the security level of the federation, additional security technology is employed to mitigate vulnerabilities in the security posture. For the present, the recommended approach is for access control of that data to be exercised by mechanisms within that federate. Future approaches may employ technology, such as a federate guard to mitigate risks.

The final check in this step is to confirm that the user needs, objectives and requirements can be met most effectively by the chosen design. Any shortfalls in this match are identified and either corrected or noted (if security related, in the SSAA) before moving on to the next step. All of this documentation, especially in the SSAA, provides the input to the formal security C&A process of the next FSP step.

The DITSCAP Initial Certification Analysis is now ready to be accomplished. This phase (Tasks 2-1 and 2-2) verifies that the previously stated architecture, software, hardware and firmware analysis complies with the federate/federation as developed. Analysis summary reports are generated.

The evaluation of the network interfaces is accomplished in Task 2-3. This evaluation is to determine whether connections to other networks or systems comply with network and overall system security policies.

The integration of software, hardware and firmware must comply with the system security architecture. The integrity of all integrated products must be maintained. Task 2-4 evaluates the integration and integrity of federations.

Life Cycle Management analysis evaluates the ability of Configuration Management (CM) to preserve the integrity of the identified security-relevant software and hardware. A report is generated summarizing the findings as part of Task 2-5.

Task 2-6 requires the Certifier to prepare written security validation procedures to be used in FSP Step 5 (DITSCAP Phase 3). These procedures include test plans and procedures.

A review of the security requirements allows the Certifier to configure the Minimum Security Checklist to meet the certification level agreed upon in previous steps.

A vulnerability assessment is performed at this time. Task 2-7 evaluates the security vulnerabilities with regard to confidentiality, integrity, availability, and accountability. It ensures that the defined threats are associated with a countermeasure that is appropriate to the level of risk associated with the federation. Results of all Phase 2 tasks are compiled, documented in the SSAA, and analyzed by the Certifier.

9.5 FSP Step 5 - Federation Integration and Test; Security Validation

Execution planning is the first activity in this step. This activity defines and develops the full set of information required to support the federation execution. Much of the supporting information is found in the Federation Execution Planners Workbook (FEPW). In addition to this workbook, members of the federation development team plan for the integration and testing of the federation, so that the execution of the federation can proceed with minimal incidents. Indeed, this planning should have been occurring all along. The documentation created and collected thus far plays an important role in determining the amount and type of integration testing which is to occur to assure seamless federation execution in a secure mode.

There can be a tremendous overlap between the testing which needs to be done to assure that the federation execution can occur without incident and the testing which needs to be done to support a positive security accreditation decision, which is required prior to execution of a federation. The planning for the testing involves all members of the team, since small modifications can have large payoffs in the use of the same test to support both areas.

For security certification, evidence is presented that supports the federation as constructed, complies with the established security requirements, and still satisfies the mission needs. It compares the as-built federation to the documentation to ensure that any security deviations, exceptions, or issues, are identified and have plans and timelines set to resolve them. This evidence is presented in the SSAA and in the results of any certification tests which are required to support a positive security accreditation decision. In addition, the certification may point to additions or modification to federation life-cycle support plans, or federation operating procedures. Often, shortfalls that are identified because of the certification test and review can be covered by changes in procedures, instead of changes in the design of the federation. However, to properly make that decision, the Certifier relies on recommendations provided by the federation security team. If this team has been fully involved in the federation development, these decisions are easy to make. If they have not been, it is likely that the decisions are not easy, and may have greater impact than is necessary.

Since the SSAA content is the basis for making the C&A decision, it is important that it be reviewed to ensure that the documentation supports the way the federation is constructed

and tested. The C&A decision consists of both the assessment of the features of the federation and the formal decision that the federation can operate in a given environment, for a specified length of time, against a particular threat environment, in a specified configuration. The amount of testing and analysis to be done that contributes to the C&A decision is documented and included in the SSAA. This can include (but is not limited to):

- Security Policy
- Penetration Testing
- TEMPEST and Red-Black Testing
- COMSEC Compliance
- System Management Analysis
- Site Survey(s)
- Contingency Planning Analysis
- Risk Management Analysis
- Configuration Audit
- Configuration Management Plan

Once the testing and analysis is defined, it is conducted. In the FEDEP, there are three levels of testing: compliance testing, integration testing and federation testing. The FSP adds security certification testing to this list. The FEDEP testing is intended to bring all the federation participants into a unifying, logical operating environment and to test that the federates can interoperate to the degree required to achieve federation objectives. Some or all of these tests can be used to support the certification evaluation. These tests can be scaled to the type of federation or federation execution being accredited for security. In addition to the functional testing and user testing of the federation, the security accreditation process requires data collection to support the accreditation decision. Just as the testing can overlap in usefulness, it is likely that data used for one purpose can be used for another.

Testing is one part of the certification analysis. An examination of the supporting documentation and plans was conducted in Task 1-1. This verified that security plans and contingencies are defined. As previously stated, a change in plans or procedures may be all that is required to correct a shortfall identified during the certification testing. However, this modification is to be made in the context of the overall plans of the federation, not in a vacuum. The change to the procedures may be simple but may lead to another shortfall. The decision on how to correct a shortfall must be carefully considered, as the procedure change may be more costly in the end than a design change in the federation.

The Security Test and Evaluation (ST&E) is used to validate the correct integration of security measures to protect the system and that the system functions as designed and is implemented in accordance with the security policies. When a system is developed for deployment to multiple locations (identical systems, software, protections and processes), a security type accreditation may be desirable. If the system is going to be type accredited, a Certification Test and Evaluation (CT&E) should occur at the central

integration and test facility. Software and hardware security tests of common system components at multiple sites are not recommended. At the conclusion of the type accreditation CT&E, the test results, Certifier's recommendation, and the type accreditation are documented in the SSAA. This SSAA is then sent with the software and hardware suite to each site where the IS is to be installed. The site need not repeat the baseline test conducted by the type accreditation effort. However, the system installation and security configuration is tested at each operational site in the sites' ST&E which becomes part of the (new) SSAA. This testing is conducted as part of Task 3-1.

Penetration testing is done as part of Task 3-2 to assess the federations' ability to withstand intentional attempts to circumvent security features by exploiting technical security vulnerabilities.

Tasks 3-3 and 3-4 validate that the site meets TEMPEST, RED-BLACK and COMSEC requirements. If COMSEC is required, a security validation is done to ensure that NSA approved procedures are in place for key management.

The system management process is analyzed to determine if system security management procedures are in place, operational and effective in Task 3-5.

A site security accreditation survey is accomplished to validate that the site is operating in conformance with the security requirements necessary to operate the federate/federation in that environment, and that no unacceptable risks to the information being processed exist (Task 3-6).

The contingency, backup and the continuity of services plans are evaluated in Task 3-7 to ensure they are consistent with operational and security requirements, and that they provide a reasonable level of continued operations if events occur that prevent normal operations.

A risk management review (Task 3-8) is accomplished before recommending security accreditation, whether positive or negative. This review analyzes the overall system security design to determine if countermeasures are adequate to limit the probability of loss or the impact of loss is reduced to an acceptable level.

The outcome of the testing is used to support the go/no-go decision of the federation sponsor, as well as to develop the recommendation to the DAA, for a go/no-go decision from the responsible security proponent. Recall that a positive decision is required before executing the federation with the real data. This decision can actually take one of three forms:

1) Full security accreditation approval, including a security re-certification/re-accreditation timeline and guidance.

2) Interim approval to operate, identifying steps that need to be completed before full security accreditation, and any controls required to be in place to compensate for any increased risk in the interim.
3) Security accreditation disapproval, including recommendations and timelines for correcting specified deficiencies.

The certification indicates that the Certifier concludes that the federation satisfies the technical requirements as specified by the applicable security policies and regulations and whether or not the federation meets the security agreements. Once that is obtained, the Certifier recommends to the DAA that the federation be security accredited to operate. Typically, the security accreditation is of a specific federation, or federation execution, within specific operational constraints, using specific procedures during operation and maintenance; all of which is included in the SSAA. It may be possible to obtain a more generic security accreditation; however, it is anticipated that the operational considerations have to be stated for all cases in which the federation is to be executed. Any operation which falls outside these cases would not be authorized under the security accreditation decision granted. This last step before execution may make clear the need for new requirements or revisions in the federation design.

9.6 FSP Step 6 - Execute and Prepare Results; Post (Security) Accreditation

If a positive security accreditation decision has been reached, step six of the FEDEP begins with the actual execution of the federation. All federation participants are now operating as an integrated whole to generate the required measures of merit and thus achieve the stated federation objectives. At this point, the FSP is in a state of monitoring and maintenance. While the execution is occurring, the security personnel at the federates, and for the federation, ensure that the execution remains within the bounds of the security accreditation. This monitoring continues until the federation is removed from service or the federation execution is completed and the data is properly disposed of or secured. Security is now a part of the normal operation of the federation.

Often there is a set of individuals (probably at least one per federate) that is responsible for ensuring that the security level of their particular federate is maintained. Usually, this occurs through monitoring the execution. This set of individuals is aware of the other factors that contributed to the positive security accreditation decision, such as mandatory security training and operational security procedures. In these procedures, it is likely that the security level of the people that interact with the federation is specified and that the environment in which the federate (or federation, depending on collocation) operates is specified. These procedures state the roles that they occupy, the training required, and the manner in which they interact with the federate and the federation. If anything falls outside the stated procedures, the responsible security individuals are to be notified. It is usually helpful for the responsible security individual to specify, either verbally, or in writing, a short checklist for all federate players to use to maintain the needed security level of the federate or federation. This individual should be readily available and make it easy for the federate or federation to operate, as well as make it easy and non-threatening

to report problems that may jeopardize the secure execution of the federation or invalidate the security accreditation decision.

One essential element of this activity in the FSP is that of configuration management. CM procedures were identified in Task 1-1. All changes to the federation, the scenario or any other supporting information or federates are monitored and controlled regardless of the security level of the federation. Each change has a potential security impact and needs to be monitored by the federation execution staff and the responsible federate security individual. These individuals are responsible for determining if, and how, the change affects the security posture of the federate and/or federation. Each change requires approval. The security representatives make recommendations based on their insights into the federation. If they have been involved in the development of the federation from the beginning, the ability to assess the impact, if any, is made easier and with more clarity. In addition, if an impact is determined, they may be able to find alternative ways to implement the same change that may make re-accreditation of the security easier. All changes, decisions, and rationale behind the decisions are to be documented in the SSAA.

The users are likewise responsible for ensuring the federation execution is conducted within the bounds of the security accreditation and as they have been instructed. The length of time for which the security accreditation is in effect may cause the users of the federation to attend periodic briefings and discussions about the security needs agreed to in the SSAA. It is expected that the security accreditation decision took into account operational and physical security factors and it is expected that these rules are followed. Participants are responsible for alerting the security personnel when something is discovered that is believed to be outside the bounds of the security accreditation. The bounds of the security accreditation, operating guidelines, training requirements, etc. can be found in the SSAA.

Security guidelines for dissolving the federation may also need to be specified and followed. The security policy, developed in the federation design task and refined in the federation development task, defines the security safeguards and the handling restrictions that are placed on the collected data, based on its designated sensitivity. The policy covers not only the process for handling the data, but also the procedures for downgrading the sensitivity of that data when appropriate. These documents can be found in the SSAA. Each federate must be aware of security concerns. Any federation specific hardware, software or data (items which do not belong to any particular federate) need to be disposed of or properly transferred according to guidance set forth in the security policy.

Phase 4 of the DITSCAP covers system operations, security operations and security compliance validation tasks that may direct the security team to repeat tasks from previous phases of the DITSCAP (FSP). These tasks are detailed in the DITSCAP Applications Manual and refer the security team to appropriate tasks depending on the level of security validation required to bring the federate or federation back to a security accredited state. When any changes are required to the federate (or federation), a reanalysis of security mechanisms is undertaken to assure that no additional vulnerabilities are introduced and

that the SSAA reflects any changes to the system baseline. These changes can occur in the system mission, threat, operating environment, security architecture or any operating procedures. If a system requires revalidation of security after the specified time period or major changes are planned for the systems, then the DITSCAP must be restarted at Phase 1.

Task 4-1 is executed whenever a change is required to the SSAA as described above. These changes are submitted to the security personnel for review and approval. After completion of this task, the process continues and a reevaluation is necessary for physical, personnel and management controls, TEMPEST and COMSEC compliance. This reevaluation occurs in Tasks 4-2 through 4-4.

Contingency Plan maintenance is accomplished in Task 4-5. Contingency plans are reviewed to ensure that they are current and provide reasonable continuity of IS support.

Configuration Management (Task 4-6) is assessed to determine whether the accepted level of residual risk is being maintained.

Task 4-7 is a review of the overall system security design, architecture and other SSAA requirements to ensure the level of risk has not changed.

The security Compliance Validation task (Task 4-8) calls for a repeat of applicable tasks found in Phases 2 and 3. The DITSCAP specifies a minimum security activity checklist that is conducted as part of this task.

IV. Conclusion

Common practice today for application of security processes, regardless of the need or application, is to delay as long as possible. While it is possible to secure a federation using this method, it is very difficult and can be needlessly costly. The FEDEP provides an opportunity to change current practice. By integrating the security process into the steps of the FEDEP and opening the dialog between the user/sponsor, the technical representatives, and the security personnel, the ability to successfully security accredit the federation, with optimal use of resources, is a very achievable endpoint. Since the security personnel are involved in the technical decisions, and vice versa, security technology and needs can be integrated almost seamlessly into the federation and provide for a smoother federation life-cycle, with higher levels of protection for the federation and its products.

The processes represented in this FSP are recommended. As in the FEDEP and DITSCAP, it is up to the users (in this case the federation members) to determine the best course of action for them. An important recommendation, however, is the early integration of the security knowledge, requirements and constraints into the federation development process. This represents the best way to effectively meet the goal of security C&A of the federation.

APPENDIX A - REFERENCES

Department of Defense (DoD) Chief Information Officer (CIO) Guidance and Policy Memorandum No. 6-8510, “Department of Defense Information Assurance”

Department of Defense Instruction 5200.40, "DoD Information Technology (IT) Security Certification and Accreditation (C&A) Process (DITSCAP) Instruction", November 30, 1999

Department of Defense Instruction 5200.40-M, "DoD Information Technology (IT) Security Certification and Accreditation (C&A) Process (DITSCAP) Application Manual", December 1999

Department of Defense Technical Architecture Framework for Information Management, Volume 6, “Department of Defense (DoD) Goal Security Architecture”, Version 3.0, Defense Information Systems Agency Center for Standards, April 30, 1996

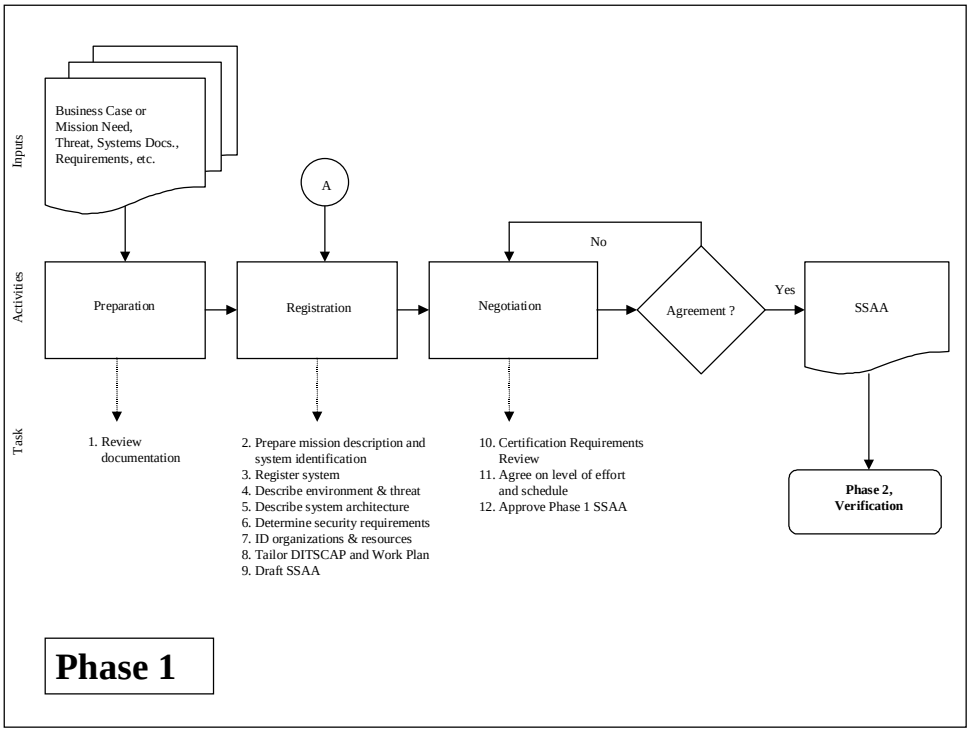
Defense Modeling and Simulation Office High Level Architecture “Federation Development and Execution Process (FEDEP) Model”, Version 1.5, December 8, 1999

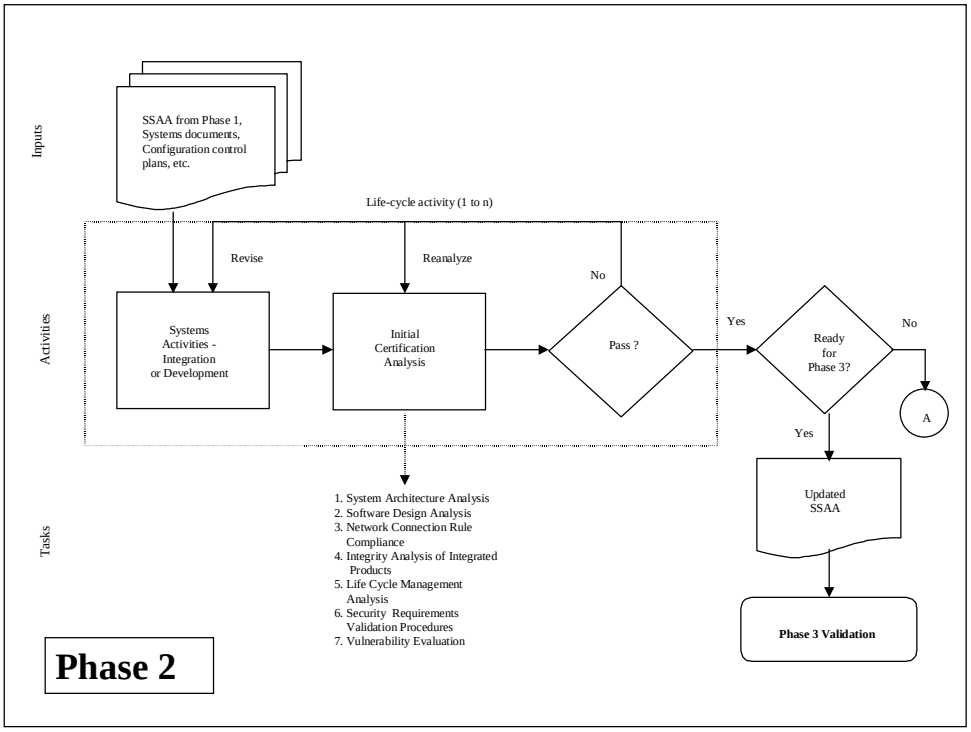
Defense Modeling and Simulation Office High Level Architecture “Federation Execution Planners Workbook (FEPW)”

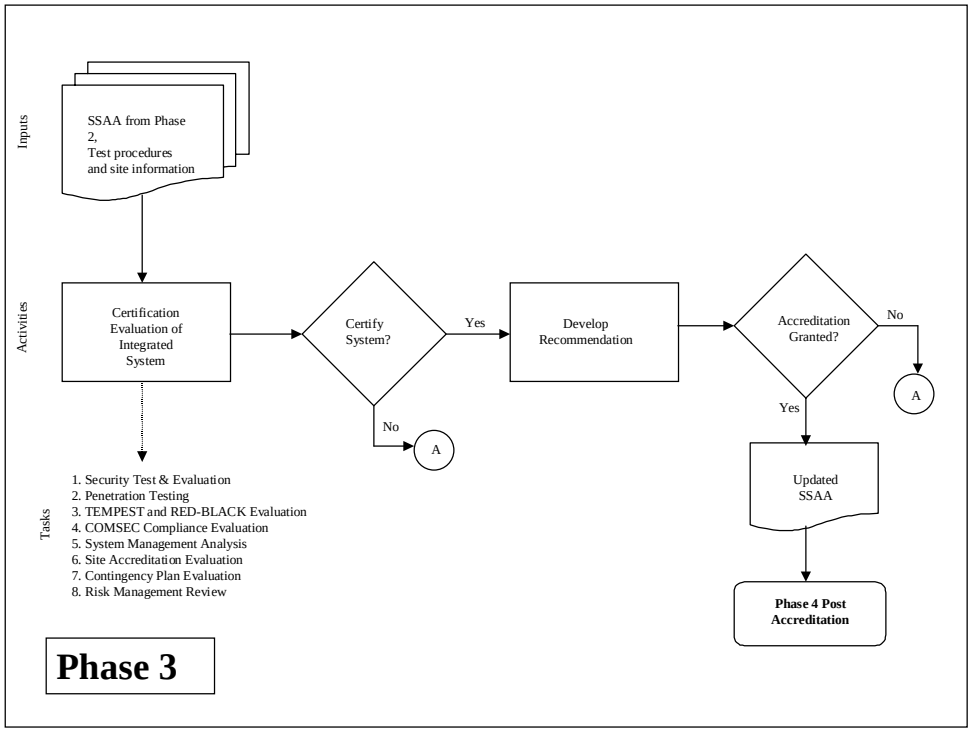
"DITSCAP Requirements Traceability Matrix (RTM) Database Users Manual", Version 1

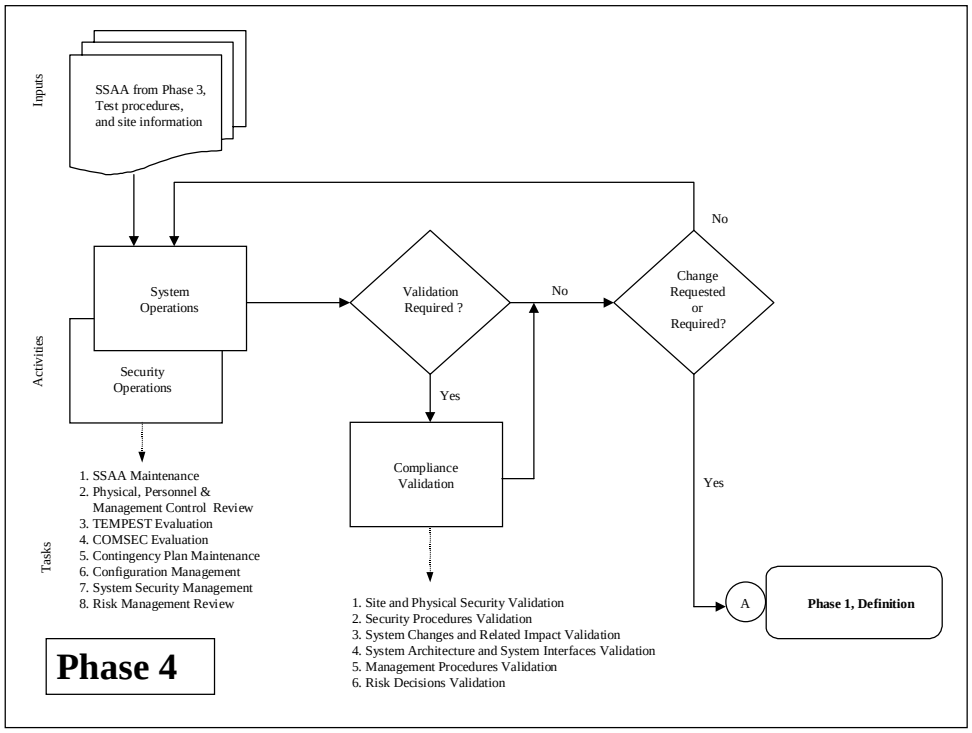
National Information Assurance Certification and Accreditation Process (NIACAP), National Security Telecommunications and Information Systems Security Committee (NISTISSC), NSTISSI No. 1000, April 2000

APPENDIX B - DITSCAP PHASES FLOWCHARTS






Inputs
SSAA from Phase 2,
Test procedures
and site information
Activities
Certification Evaluation of Integrated System
Certify System?
Yes
No
A
Develop Recommendation
Accreditation Granted?
No
A
Yes
Updated SSAA
Phase 4 Post Accreditation
Tasks
1. Security Test & Evaluation
2. Penetration Testing
3. TEMPEST and RED-BLACK Evaluation
4. COMSEC Compliance Evaluation
5. System Management Analysis
6. Site Accreditation Evaluation
7. Contingency Plan Evaluation
8. Risk Management Review
Phase 3


Inputs
SSAA from Phase 3,
Test procedures,
and site information
Activities
System Operations
Security Operations
Validation Required ?
No
Change Requested or Required?
No
Yes
Compliance Validation
Yes
A
Phase 1, Definition
Tasks
1. SSAA Maintenance
2. Physical, Personnel & Management Control Review
3. TEMPEST Evaluation
4. COMSEC Evaluation
5. Contingency Plan Maintenance
6. Configuration Management
7. System Security Management
8. Risk Management Review
1. Site and Physical Security Validation
2. Security Procedures Validation
3. System Changes and Related Impact Validation
4. System Architecture and System Interfaces Validation
5. Management Procedures Validation
6. Risk Decisions Validation
Phase 4

APPENDIX C – SAMPLE FEDERATIONS

Sample Level 1 Federation

This sample illustrates a federation operating with no interfaces (interface mode = benign) in a dedicated mode processing sensitive only data (information category = sensitive) with each user having a valid security clearance for all information within the system (processing mode = dedicated). Some processing, storage or data carries a need to attribute it to users or processes. The mission is partially dependant (mission-reliance = partial) on the specific operation, data, infrastructure or system. The system must be available in a reasonable amount of time (availability = reasonable) to avoid operational impacts. The degree of integrity is irrelevant (integrity = not applicable) as to operational impacts.

Sample Level 2 Federation

This sample illustrates a federation operating with indirect interaction (receive only from sensors) to other systems (interface mode = passive). The federation runs in system high mode (processing mode = system high) with each user having a valid security clearance for all information and a need-to-know for some of this information. All or almost all of the processing, transmission, storage or data carries the need to attribute it to users or processes (attribution mode = comprehensive). The mission is partially dependant (mission reliance = partial) on the operation, data, infrastructure or system and must be available in a reasonable amount of time to avoid operational impacts (availability = reasonable). The degree of integrity is irrelevant to the operational impacts (integrity = not applicable). The system operates at the Top Secret level (information category = Top Secret).

Sample Level 3 Federation

This sample illustrates a federation actively interfacing (interface mode = active) with other systems over the SIPRNET , operating at system high (processing mode = system high) and processing data at the Top Secret (information category = Top Secret) level. All or almost all data must be attributed to a user or process (attribution mode = comprehensive). This federation mission is totally dependant on the operation, data, infrastructure or system (mission-reliance = total). The system must be available as soon as possible to avoid operational impacts (availability = ASAP). The degree of integrity must be approximate in order to avoid operational impacts (integrity = approximate).

Sample Level 4 Federation

This sample illustrates a federation actively interfacing with the SIPRNET and NIPRNET (interface mode = active), operating in a multi-level mode (processing mode = multi-level) and processing Top Secret (information category = Top Secret) data. All or almost all data must be attributed to a user or process (attribution mode = comprehensive). The mission is totally dependent on the operation, data, infrastructure or system (mission-reliance = total). The system must be available on demand (availability = immediately) to

prevent operational impacts. The degree of integrity must be exact (integrity = exact) to avoid operational impacts.

Using the table below (from the DITSCAP Application Manual) we can calculate the total weights of all characteristics of the federation under development to determine the level of certification required.

Characteristic	Alternatives and Weights	Weight
Interfacing Mode	Benign (w=0), Passive (w=2), Active (w=6)	
Processing Mode	Dedicated (w=1), System High (w=2), Compartmented (w=5), Multilevel (w=8)	
Attribution Mode	None (w=0), Rudimentary (w=1), Selected (w=3) Comprehensive (w=6)	
Mission-Reliance	None (w=0), Cursory (w=1), Partial (w=3), Total (w=7)	
Availability	Reasonable (w=1), Soon (w=2), ASAP (w=4) Immediate (w=7)	
Integrity	Not-applicable (w=0), Approximate (w=3), Exact (w=6)	
Information Categories	Unclassified (w=1), Sensitive (w=2), Confidential (w=3), Secret (w=5), Top Secret (w=6), Compartmented/Special Access Classified (w=8)	
Total of all weights		

Table 4: CERTIFICATION LEVEL CHARACTERISTICS

Characteristic	Level 1 Federation	Level 2 Federation	Level 3 Federation	Level 4 Federation
Interfacing Mode	0	2	6	6
Processing Mode	1	2	2	8
Attribution Mode	3	6	6	6
Mission-Reliance	3	3	7	7
Availability	1	1	4	7
Integrity	0	0	3	6
Information Categories	2	6	6	6
Total weight	**11**	**20**	**34**	**46**

Table 5: SAMPLE SYSTEMS CALCULATED CERTIFICATION LEVELS

APPENDIX D – DITSCAP ROLES AND RESPONSIBILITIES

	Mgmt. Roles	Security Roles		User Roles
Phase	**Program Manager**	**DAA**	**Certifier**	**User Rep.**
Phase 1	• Initiate security dialogue with DAA, Certifier, and user representative • Define system schedule and budget • Support DITSCAP tailoring and level of effort determination • Define system architecture • Prepare Life Cycle Management Plans • Define security architecture	• Define accreditation requirements • Obtain threat assessment • Assign the Certifier • Support DITSCAP tailoring • Approve the SSAA	• Begin vulnerability and risk assessments • Review threat definition • Lead DITSCAP tailoring • Determine level of certification effort • Describe certification team roles and responsibilities • Draft SSAA	• Support DITSCAP tailoring and level of effort determination • Define operational needs in terms of mission • Identify vulnerabilities to mission • Define operational resource constraints
Phase 2	• Develop system or system modifications • Support certification activities • Review certification results • Revise system as needed • Resolve security discrepancies	• Support certification activities	• Conduct certification activities • Assess vulnerabilities • Report results to the program manager, DAA, and user representative • Determine if system is ready for certification • Update the SSAA	• Prepare security Rules of Behavior (ROB) and Standard Operating Procedures (SOP) • Support certification actions

Phase	Mgmt. Roles	Security Roles		User Roles
	Program Manager	**DAA**	**Certifier**	**User Rep.**
Phase 3	• Support certification activities • Provide IS access for ST&E • Provide system corrections under configuration management	• Assess vulnerabilities and residual risk • Decide to accredit, IATO, or terminate system operations	• Conduct certification activities • Evaluate security requirements compliance • Assess vulnerabilities and residual risk • Report results to the program manager, DAA, and user representative • Recommend risk mitigation measures • Prepare final SSAA • Recommend accreditation type	• Support certification efforts • Implement and maintain SOP and ROB • Review certification results
Phase 4	• Update IS to address Phase 3 reported vulnerabilities and patches under configuration management • Report security related changes to the IS to the DAA and user representative • Review and update life cycle management policies and standards • Resolve security discrepancies	• Review the SSAA • Review proposed changes • Oversee compliance validation • Monitor C&A integrity • Decide to reaccredit, accredit, IATO, or, if SSAA is no longer valid, terminate system operations		• Report vulnerability and security incidents • Report threats to mission environment • Review and update system vulnerabilities • Review and change security policy and standards • Initiate SSAA review if changes to threat or system

APPENDIX E – DITSCAP TASKS

PHASE 1 – DEFINITION

Preparation

1-1 Review Documentation
Obtain and review documentation (Business Case, Mission Needs Statement, System Specifications, Architecture and Design Documents, User Manuals, Operating Procedures, Network Diagrams, Configuration Management Documents, Threat Analysis, and Federal and Agency or Service IA and security instructions and policies)
Responsibility - Certifier
Produces – SSAA Outline

Registration

1-2 Prepare the System and Functional Description and System Identification
Prepare an accurate description of the system. Define system mission, function, capabilities, CONOPS, boundaries, criticality, classification and sensitivity of data (classification, SCI, special handling requirements, type of information processed and security clearances required by position held) and the system life cycle.
Responsibility - User Representative
Produces – SSAA Section 1

1-3 Register the System - Certifier
Identify the agencies and individuals (DAA, Certifier, Program Manager and user representative) involved in the C&A process and determine the current status of the system.
Responsibility - Certifier
Produces – Notification to authorities of system status

1-4 Prepare the Environment and Threat Description
Define the system environment and potential threats to the system. Operating environment security involves the facility security, physical security, administrative security, personnel security, COMSEC requirements, TEMPEST requirements, preventive maintenance and security training. Describe the security strategy to be used when developing, integrating and maintaining the security of the operating environment. Potential threats and their expected frequency to the security of the system must be identified, the risk associated with each must be evaluated and cost-effective countermeasures must be identified to mitigate the risk.
Responsibility - Certifier
Produces – SSAA Section 2

1-5 Determine the System Security Requirements

Identify system security requirements based on applicable directives, requirements and instructions. Determine the type of data processed and applicable security requirements. The security CONOPS, TFM or Security Features User's Guide (SFUG) should be included in the SSAA. Determine the network connection rules, configuration management requirements, and reaccreditations requirements. Produce the RTM.
Responsibility - Certifier
Produces – SSAA Section 4

1-6 Prepare the System Architecture Description
Define the system hardware, software, firmware, interfaces, data flows and the accreditation boundary.
Responsibility - Certifier
Produces – SSAA Section 3

1-7 Identify the C&A Organizations and the Resources Required
Identify the organizations, resources, training requirements, other supporting organizations and individuals involved in the C&A process.
Responsibility – Program Manager, DAA and User Representative
Produces – SSAA Section 5

1-8 Tailor the DITSCAP and Prepare the DITSCAP Plan
Determine the appropriate certification level and adjust the DITSCAP activities to the program strategy and system life cycle. By examining seven system characteristics and associating a weight (value) to each, the required certification level is determined. Tailor the DITSCAP by examining programmatic considerations, the security environment and the IS characteristics. Prepare the DITSCAP plan that documents the tailoring and defines the activities required for the C&A process.
Responsibility - Certifier
Produces – SSAA Section 6

1-9 Draft the SSAA
Certification team completes and assembles the SSAA document. This draft SSAA is delivered to the DAA, Certifier, program manager and user representative for review.
Responsibility – Certifier or Program Manager
Produces – Draft Phase 1 SSAA

Negotiation

1-10 Conduct Certification Requirements Review (CRR)
DAA, Certifier, program manager and user representative discuss system functionality, security requirements, level of effort and the planned C&A schedule.
Responsibility – DAA, Certifier, Program Manager, User Representative

Produces – Agreement regarding the level of effort and approach to implement security requirements

1-11 Establish Agreement on Level of Effort and Schedule

Ensure that all representatives agree on the level of effort and the schedule for the C&A activities.

Responsibility – DAA, Certifier, Program Manager, User Representative
Produces – Agreement of scheduled activities

1-12 Approve Phase 1 SSAA

Obtain the approval of the DDA for Phase 1 SSAA.

Responsibility – DAA, Certifier, Program Manager, User Representative
Produces – Approved SSAA

PHASE 2 – VERIFICATION

Refine the SSAA

Responsibility – Certifier

System Development and Integration

Responsibility - Program Manager

Initial Certification Analysis

2-1 System Architecture Analysis

Verify that the system and security architecture matches the SSAA description of the architecture. Complete the minimal security checklist for all levels of certification and any additional evaluations for certification levels 2-4.

Responsibility - Certifier

Produces – System Architecture Analysis Summary Report containing:

1) **record of findings**
2) **evaluation of vulnerabilities discovered during evaluations**
3) **summary of the analysis level of effort**
4) **summary of tools used and results obtained**
5) **recommendations**

2-2 Software, Hardware and Firmware Design Analysis

Assess the software, hardware and firmware security architecture for compliance with the requirements in the SSAA and the security architecture of the system. Complete the minimal security checklist and any additional tasks associated with certification levels 2-4.

Responsibility - Certifier

Produces – Software, Hardware and Firmware Analysis Summary Report containing:

1) **record of findings**
2) **evaluation of vulnerabilities discovered during evaluations**
3) **summary of the analysis level of effort**
4) **summary of tools used and results obtained**
5) **recommendations**

2-3 Network Connection Rule Compliance Analysis

Evaluate connections to other systems and/or networks to ensure that network and overall system security policies are enforced. Complete the minimal security checklist and any additional tasks associated with certification levels 2-4.

Responsibility - Certifier

Produces – Network Compliance Summary Report containing:

1) **record of findings**
2) **evaluation of vulnerabilities discovered during evaluations**
3) **summary of the analysis level of effort**

4) **summary of tools used and results obtained**
5) **recommendations**

2-4 Integrity Analysis of Integrated Products

Evaluate the integration of all software, hardware and firmware to ensure compliance with the system security architecture and that the integrity of each product is maintained. Complete the minimal security checklist and any additional tasks associated with certification levels 2-4.

Responsibility - Certifier

Produces – Integrated Product Analysis Summary Report containing:

1) **record of findings**
2) **evaluation of vulnerabilities discovered during evaluations**
3) **summary of the analysis level of effort**
4) **summary of tools used and results obtained**
5) **recommendations**

2-5 Life Cycle Management Analysis

Evaluate the ability of configuration management (CM) to preserve the integrity of the identified security-relevant software and hardware. Complete the minimal security checklist and any additional tasks associated with certification levels 2-4.

Responsibility – Certifier

Produces – Life Cycle Management Analysis Summary Report containing:

1) **record of findings**
2) **evaluation of vulnerabilities discovered during evaluations**
3) **summary of the analysis level of effort**
4) **summary of tools used and results obtained**
5) **recommendations**

2-6 Security Requirements Validation Procedures

Prepare the written requirements validation procedures to be used in Phase 3 to validate compliance with the technical security requirements. Perform specific tasks associated with the certification level assigned to the system as specified in the DITSCAP Application Manual.

Responsibility – Certifier

Produces – Customized Minimum Security Checklist, Test Plans and Procedures

2-7 Vulnerability Assessment

Evaluate the security vulnerabilities with regard to confidentiality, integrity, availability and accountability. Ensure that the recommended countermeasures to defined threats are appropriate to the level of risk associated with the system. Complete the minimal security checklist and any additional tasks associated with certification levels 2-4.

Responsibility – Certifier

Produces – Vulnerability Assessment Report

Analyze Results

Responsibility - Certifier

PHASE 3 – VALIDATION

Refine SSAA

Responsibility - Certifier

Certification Evaluation of Integrated System

3-1 Security Test and Evaluation (ST&E)

Validate the correct integration of security measures to protect the system, function as designed and implemented in accordance with the SSAA. Complete the minimal security checklist and any additional tasks associated with certification levels 2-4. If the system is going to be type accredited, a Certification Test and Evaluation (CT&E) should occur at the central integration and test facility.

Responsibility - Certifier

Produces – ST&E Analysis Summary Report containing:

1) **Record of findings**
2) **Evaluation of vulnerabilities discovered during evaluations**
3) **Summary of the analysis level of effort**
4) **Summary of tools used and results obtained**
5) **Recommendations**

3-2 Penetration Testing

Assess the system's ability to withstand intentional attempts to circumvent system security features by exploiting technical security vulnerabilities. Complete the minimal security checklist and any additional tasks associated with certification levels 2-4.

Responsibility - Certifier

Produces – Penetration Testing Analysis Summary Report containing:

1) **Record of findings**
2) **Evaluation of vulnerabilities discovered during evaluations**
3) **Summary of the analysis level of effort**
4) **Summary of tools used and results obtained**
5) **Recommendations**

3-3 TEMPEST and RED-BLACK Verification

If TEMPEST is required, validate that the site meets the TEMPEST and RED-BLACK requirements. Complete tasks associated with certification levels 2-4.

Responsibility - Certifier

Produces – TEMPEST/RED-BLACK Analysis Summary Report containing:

1) **Record of findings**
2) **Evaluation of vulnerabilities discovered during evaluations**
3) **Summary of the analysis level of effort**
4) **Summary of tools used and results obtained**
5) **Recommendations**

3-4 COMSEC Compliance Verification

If COMSEC is required, validate that the appropriate NSA approved COMSEC is in use and approval has been granted. Ensure that COMSEC key management procedures are in place. Complete tasks associated with certification levels 2-4.

Responsibility - Certifier

Produces – COMSEC Analysis Summary Report containing:

1) **Record of findings**
2) **Evaluation of vulnerabilities discovered during evaluations**
3) **Summary of the analysis level of effort**
4) **Summary of tools used and results obtained**
5) **Recommendations**

3-5 System Management Analysis

Validate that the system security management procedures are in place, operational and effective. CM policies must consider security implications in the accredited system baseline and operational concept. Complete the minimal security checklist and any additional tasks associated with certification levels 2-4.

Responsibility – Certifier

Produces – System Management Analysis Summary Report containing:

1) **Record of findings**
2) **Evaluation of vulnerabilities discovered during evaluations**
3) **Summary of the analysis level of effort**
4) **Summary of tools used and results obtained**
5) **Recommendations**

3-6 Site Accreditation Survey

Validate that the site operation of the IS is accomplished as documented in the SSAA to determine if it poses any unacceptable risks to the information being processed. Complete the minimal security checklist and any additional tasks associated with certification levels 2-4.

Responsibility - Certifier

Produces – Site Accreditation Survey Analysis Summary Report containing:

1) **Record of findings**
2) **Evaluation of vulnerabilities discovered during evaluations**
3) **Summary of the analysis level of effort**
4) **Summary of tools used and results obtained**
5) **Recommendations**

3-7 Contingency Plan Evaluation

Evaluate the contingency, backup and continuity of service plans to ensure they are consistent with the requirements identified in the SSAA and that they provide reasonable continuity of IS support if events occur that prevent normal operations. Complete the minimal security checklist and any additional tasks associated with certification levels 2-4.

Responsibility - Certifier

Produces – Contingency Plan Analysis Summary Report containing:

1) **Record of findings**
2) **Evaluation of vulnerabilities discovered during evaluations**
3) **Summary of the analysis level of effort**
4) **Summary of tools used and results obtained**
5) **Recommendations**

3-8 Risk Management Review

Analyze the overall system security design to determine if countermeasures are adequate to limit the probability of loss or the impact of loss is reduced to an acceptable level. Complete the minimal security checklist and any additional tasks associated with certification levels 2-4.

Responsibility - Certifier

Produces – Risk Management Analysis Summary Report containing:

1) **Record of findings**
2) **Evaluation of vulnerabilities discovered during evaluations**
3) **Summary of the analysis level of effort**
4) **Summary of tools used and results obtained**
5) **Recommendations**

Accreditation Recommendation

Responsibility - Certifier

Accreditation Decision

Responsibility - DAA

PHASE 4 – POST ACCREDITATION

System Operations

Security Operations

4-1 SSAA Maintenance

Update the SSAA whenever any change occurs to the system mission, threat, operating environment, security architecture or operating procedure. Changes are submitted to the DAA, program manager and user representative for approval.

Responsibility – User Representative, ISSO

Produces – A revised SSAA

4-2 Physical, Personnel and Management Control Review

Review physical, personnel and management controls to ensure continued compliance with the SSAA and to ensure they pose no unacceptable risks to the information being processed. Complete the minimal security checklist and any additional tasks associated with certification levels 2-4.

Responsibility – User Representative, ISSO

Produces - Physical, Personnel and Management Control Review Summary Report containing:

1) **Record of findings**
2) **Evaluation of vulnerabilities discovered during evaluations**
3) **Summary of the analysis level of effort**
4) **Summary of tools used and results obtained**
5) **Recommendations**

4-3 TEMPEST Evaluation

Validate that the equipment and site continue to meet TEMPEST and RED-BLACK requirements, if appropriate. Complete tasks associated with certification levels 2-4.

Responsibility – User Representative, ISSO

Produces – TEMPEST Evaluation Summary Report containing:

1) **Record of findings**
2) **Evaluation of vulnerabilities discovered during evaluations**
3) **Summary of the analysis level of effort**
4) **Summary of tools used and results obtained**
5) **Recommendations**

4-4 COMSEC Compliance Evaluation

Validate that COMSEC approval has been granted, approved key management procedures continue to be used and that COMSEC continues to support the requirements and agreements in the SSAA. Complete tasks associated with certification levels 2-4.

Responsibility – User Representative, ISSO

Produces – COMSEC Compliance Evaluation Summary Report containing:

1) **Record of findings**
2) **Evaluation of vulnerabilities discovered during evaluations**
3) **Summary of the analysis level of effort**
4) **Summary of tools used and results obtained**
5) **Recommendations**

4-5 Contingency Plan Maintenance

Periodically review contingency plans to ensure that they remain current and continue to provide reasonable continuity of IS support when events occur that prevent normal operations. Complete the minimal security checklist and any additional tasks associated with certification levels 2-4.

Responsibility – User Representative, ISSO

Produces - Contingency Plan Maintenance Summary Report containing:

1) **Record of findings**
2) **Evaluation of vulnerabilities discovered during evaluations**
3) **Summary of the analysis level of effort**
4) **Summary of tools used and results obtained**
5) **Recommendations**

4-6 Configuration Management

Assess proposed changes to the accredited system to ensure that an acceptable level of residual risk is maintained. Complete tasks associated with certification levels 1-4.

Responsibility – User Representative, ISSO

Produces - Configuration Management Summary Report containing:

1) **Record of findings**
2) **Evaluation of vulnerabilities discovered during evaluations**
3) **Summary of the analysis level of effort**
4) **Summary of tools used and results obtained**
5) **Recommendations**

4-7 Risk Management Review

Review the overall system security design, architecture, and other SSAA requirements against the concept of operations, operational environment, and threats to ensure that risk to confidentiality, integrity, availability, or accountability of the information and system remains acceptable. Complete the minimal security checklist and any additional tasks associated with certification levels 2-4.

Responsibility – User Representative, ISSO

Produces – Updated SSAA and a Risk Management Review Summary Report containing:

1) **Record of findings**
2) **Evaluation of vulnerabilities discovered during evaluations**
3) **Summary of the analysis level of effort**
4) **Summary of tools used and results obtained**

5) **Recommendations**

4-8 Compliance Validation

Ensure that the contents of the SSAA adequately address the functional environment into which the IS has been placed and that the IS complies with the SSAA. This task should repeat all applicable Phase 2 and 3 tasks. Complete the minimal security checklist and any additional tasks associated with certification levels 2-4.

Responsibility – Certifier, ISSO, DAA

Produces - Compliance Validation Summary Report containing:

1) **Record of findings**
2) **Evaluation of vulnerabilities discovered during evaluations**
3) **Summary of the analysis level of effort**
4) **Summary of tools used and results obtained**
5) **Recommendations**

APPENDIX F – SSAA OUTLINE

1.0 MISSION DESCRIPTION AND SYSTEM IDENTIFICATION

- 1.1 System Name and Identification
- 1.2 System Description
- 1.3 Functional Description
  - 1.3.1 System Capabilities
  - 1.3.2 System Criticality
  - 1.3.3 Classification and Sensitivity of Data Processed
  - 1.3.4 System User Description and Clearance Levels
  - 1.3.5 Life Cycle of the System
- 1.4 System CONOPS Summary

2.0 ENVIRONMENT DESCRIPTION

- 2.1 Operating Environment
  - 2.1.1 Facility Description
  - 2.1.2 Physical Security
  - 2.1.3 Administrative Issues
  - 2.1.4 Personnel
  - 2.1.5 COMSEC
  - 2.1.6 TEMPEST
  - 2.1.7 Maintenance Procedures
  - 2.1.8 Training Plans
- 2.2 Software Development and Maintenance Environment
- 2.3 Threat Description

3.0 SYSTEM ARCHITECTURAL DESCRIPTION

- 3.1 System Architecture Description
- 3.2 System Interfaces and External Connections
- 3.3 Data Flow
- 3.4 Accreditation Boundary

4.0 SYSTEM SECURITY REQUIREMENTS

- 4.1 National and DoD Security Requirements
- 4.2 Governing Security Requisites
- 4.3 Data Security Requirements
- 4.4 Security CONOPS
- 4.5 Network Connection Rules
- 4.6 Configuration Management Requirements
- 4.7 Reaccreditation Requirements

5.0 ORGANIZATIONS AND RESOURCES

- 5.1 Organizations
- 5.2 Resources
- 5.3 Training

5.4 Other Supporting Organizations

6.0 DITSCAP PLAN

6.1 Tailoring Factors
- 6.1.1 Programmatic Considerations
- 6.1.2 Security Environment
- 6.1.3 IS Characteristics
- 6.1.4 Reuse of Previously Approved Solutions

6.2 Tasks and Milestones
6.3 Schedule Summary
6.4 Level of Effort
6.5 Roles and Responsibilities

AP1.1.2 Appendices. Appendices should include system C&A artifacts. Optional appendices may be added to meet specific needs. Include all documentation that is relevant to the C&A process.

Appendix A	Acronyms
Appendix B	Definitions
Appendix C	References
Appendix D	System Concept of Operations
Appendix E	Information System Security Policy
Appendix F	Security Requirements and/or Requirements Traceability Matrix
Appendix G	Certification Test and Evaluation Plan and Procedures (Type only)
Appendix H	Security Test and Evaluation Plan and Procedures
Appendix I	Applicable System Development Artifacts or System Documentation
Appendix J	System Rules of Behavior
Appendix K	Incident Response Plan
Appendix L	Contingency Plans
Appendix M	Personnel Controls and Technical Security Controls
Appendix N	Memorandums of Agreement – System Interconnect Agreements
Appendix O	Security Education, Training, and Awareness Plan
Appendix P	Test and Evaluation Report(s)
Appendix Q	Residual Risk Assessment Results
Appendix R	Certification and Accreditation Statements

APPENDIX G - ACRONYMS

AIS – Automated Information System
ASAP – As soon as possible
C&A – (Security) Certification and Accreditation
CM – Configuration Management
COMSEC – Communications Security
CONOPS – Concept of Operations
CRR – Certification Requirements Review
CT&E – Certification Test and Evaluation
DAA – Designated Approving Authority
DITSCAP – Department of Defense Information Technology Security Certification and Accreditation Process
DMSO – Defense Modeling and Simulation Office
DoD – Department of Defense
FCM – Federation Conceptual Model
FEDEP – Federation Development and Execution Process
FEPW – Federation Execution Planners Workbook
FOM – Federation Object Model
FSP – Federation Security Process
FSS – Federation Scenario Specification
HLA – High Level Architecture
IA – Information Assurance
IATO – Interim Authority to Operate
IS – Information System
ISSO – Information System Security Officer
LAN – Local Area Network
MSRR – Modeling and Simulation Resource Repository
NIPRNET - Unclassified (but Sensitive) Internet Protocol Routing Network
NISTISSC - National Security Telecommunications and Information Systems Security Committee
NSTISSI - National Security Telecommunications and Information Systems Security Instruction
NIACAP - National Information Assurance Certification and Accreditation Process
OMT – object model template
ROB – Rules of Behavior
RTI – Runtime Infrastructure
RTM – Requirements Traceability Matrix
SFUG – Security Features User's Guide
SIPRNET – Secret Internet Protocol Routing Network
SOP – Standard Operating Procedure
SSAA – System Security Authorization Agreement
ST&E – Security Test and Evaluation
TFM – Trusted Facilities Manual
VV&A – Verification, Validation and Accreditation